EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Michael Chan (Reg. No. 33663) on 01/27/2009.

The application has been amended as follows:

21. (Currently Amended) A method of operating a portable computer, comprising:

a) storing records of events experienced by the computer in user-accessible memory within the computer;

b) using one or more of the records as seed for generating plain text of a first session key K1, wherein

(A) a hashing algorithm is applied to the seed to provide a hashed value which is split into two portions and

(B) the two portions are processed to provide K1; and then

c) encrypting K1, transmitting K1(encrypted) to an external terminal, receiving an encrypted response from the external terminal, and de-crypting the encrypted response using the plain text of K1.

24. (Currently Amended) A method, comprising:

a) using a portable computer to

i) generate a first session key K1, based on one or more seeds derived from data contained in user-accessible memory, wherein

(A) a hashing algorithm is applied to the one or more seeds to provide a hashed value which is split into two portions and

(B) the two portions are processed to provide K1;

ii) encrypt K1 into K1(encrypted), using a public key PK;

iii) transmitting K1(encrypted) to an external terminal in connection with a first transaction;

b) using the portable computer to

i) generate a second session key K2, based on one or more seeds derived from data contained in user-accessible memory, wherein

(A) a hashing algorithm is applied to the one or more seeds to provide a hashed value which is split into two portions and

(B) the two portions are processed to provide K2;

ii) encrypt K2 into K2(encrypted), using a the public key PK;

iii) transmitting K2(encrypted) to an external terminal in connection with a second transaction.

28. (Currently Amended) A method, comprising:

a) maintaining a commercially available Personal Digital Assistant, PDA, which has no secure area for storing an encryption key usable to encrypt outgoing data; and

b) using the PDA for encryption and transmission of a message to an external controller in connection with a financial transaction, wherein the encryption comprises deriving a seed from data stored in user-accessible memory; and deriving a session key from said seed, which session key is used in the financial transaction, and not used thereafter, wherein

(A) a hashing algorithm is applied to the seed to provide a hashed value which is split into two portions and

(B) the two portions are processed to provide the session key.

29. (Canceled).

30. (Currently Amended) Apparatus, comprising:

a) a portable computer having

i) no secure area for storing an encryption key used to encrypt outgoing data;

ii) system memory, all of which is accessible to a user of the computer; and

iii) data stored in the system memory, which data changes over time;

b) means for

i) utilizing selected changing data in the system memory as a seed for generating a session key K1, wherein

(A) a hashing algorithm is applied to the seed to provide a hashed value which is split into two portions and

(B) the two portions are processed to provide K1;

ii) encrypting K1 into K1(encrypted) ; and

iii) transmitting K1(encrypted) to an external terminal.

33. (Currently amended) A portable computer, comprising:

a) means for storing records of events experienced by the computer in user-accessible memory within the computer;

b) means for using one or more of the records as a seed for generating an encryption key, wherein

(A) a hashing algorithm is applied to the seed to provide a hashed value which is split into two portions and

(B) the two portions are processed to provide the encryption key; and

c) means for using the encryption key in a transaction with an external terminal.

38. (Currently amended) A method, comprising:

a) storing records of events experienced by a portable computer in user-accessible memory within the computer;

b) using one or more of the records as a seed for generating a session key K1, wherein

(A) a hashing algorithm is applied to the seed to provide a hashed value which is split into two portions and

(B) the two portions are processed to provide K1;

c) encrypting K1 into K1(encrypted) using a public key;

d) transmitting K1(encrypted) to an external terminal;

e) at the external terminal, decrypting K1(encrypted) into K1;

f) encrypting a message M into M(encrypted) using K1 as key;

g) transmitting M(encrypted) to the portable computer; and

h) decrypting M(encrypted) using K1 within the portable computer.

Allowable Subject Matter

2. Claims 21-28 and 30-38 are allowed.

3. The following is an examiner's statement of reasons for allowance: The prior art teaches generating a key based on a seed created from records of a system and to use this key to encrypt and decrypt message. However, the prior art fails to teach the steps of applying a hashing algorithm to the seed to provide a hashed value which is split into two portions and the two portions are processed to provide the key in combination with the remaining claimed limitations.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

4. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Roden teaches generating a session key in a first device, encrypting it for transport to a second device; decrypting the session key; and using the session key to encrypt and decrypt messages sent between the two devices.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL PYZOCHA whose telephone number is (571)272-3875. The examiner can normally be reached on Monday-Thursday, 7:00am - 4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. P./
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437